IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
BLACK CLOUD MOBILE CELLULAR PHONE (**TARGET DEVICE**)	Magistrate No. 24-1258

AFFIDAVIT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS IN SUPPORT OF A SEARCH WARRANT

I, Samantha Keener, being duly sworn, depose and state as follows:

I. INTRODUCTION AND PURPOSE OF THIS AFFIDAVIT

1. This is an Affidavit provided in support of an application for a search warrant pursuant Federal Rule of Criminal Procedure 41. Specifically, I seek a search and seizure warrant authorizing the search and seizure of the following cellular telephone/electronic devices ("**TARGET DEVICE**"), which was seized inside of 304 Kathleen St., Pittsburgh, PA 15211, belonging to Cayce WILLIAMS ("WILLIAMS"):

> **TARGET DEVICE 1**: Black Cloud Mobile cellular phone; recovered from the entertainment center, next to the television, inside of the living room of 304 Kathleen St., Pittsburgh, PA 15211, on July 19, 2024.

2. A search warrant for the **TARGET DEVICE** is being sought as part of an investigation into CAYCE WILLIAMS, Malik MARTINEZ and other members and associates of a Drug Trafficking Organization, who are responsible for distributing quantities of crack cocaine and heroin and/or fentanyl in the Western District of Pennsylvania. This application and affidavit are submitted in support of a search warrant for the **TARGET DEVICE** described below, associated with WILLIAMS. Accordingly, law enforcement has probable cause to believe that a search of this phone will produce fruits of, or evidence of, violations of federal felony offenses 21 U.S.C. §§ 841(a)(1) and 841(b)(1)(C) (knowingly, intentionally, and unlawfully possessing with

intent to distribute a quantity of cocaine base, and a quantity of fentanyl, each of which is a Schedule II controlled substance). Collectively, these offenses will be referred to as the "TARGET OFFENSES" below. As explained further below, there is probable cause to believe that evidence of violations of the TARGET OFFENSES will be found within the **TARGET DEVICE**.

3. The warrant would authorize the forensic examination of the **TARGET DEVICE** for the purpose of identifying electronically stored data particularly described in Attachment B and using the protocols described in Attachment B by members of the FBI, or their authorized representatives, including but not limited to other law enforcement agents assisting the above-described investigation. The **TARGET DEVICE** was originally seized by state law enforcement officers on July 19, 2024, and remained in secure law enforcement custody from those days. Based on my training and experience, I know that the **TARGET DEVICE** has been stored in a manner substantially the same state as it was when the device first came into the possession of law enforcement.

II. BACKGROUND OF SPECIAL AGENT KEENER

4. I am a Special Agent ("SA") of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and have been so employed since September 2021. Since February 2022, I have been assigned to the Pittsburgh Division. During that time, I have become familiar with methods and techniques associated with investigations into organized crime, drug trafficking, gangs, and violent crimes. My experience as an FBI Special Agent has included the investigation of cases involving drug crimes, firearms violations, and I have enforced federal laws prohibiting these offenses.

5. As a Special Agent with the FBI, I am an "Investigative or Law Enforcement Officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7);

that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

6. I have been involved in many narcotics-related arrests and the service of many narcotics-related search warrants. I have handled cooperating sources of information who were involved in narcotics acquisition and/or trafficking. In addition, I have reviewed many communications between drug traffickers as a result of my participation in multiple wiretap investigations. As a result of my narcotics-related training and experience, I am familiar with the methods and language used to distribute narcotics, to launder proceeds, and to operate drug-trafficking conspiracies.

7. Based upon my training, knowledge, and experience, I know that cellular telephones are capable of storing information including, but not limited to, text and audio communications, call history, contact information, calendar entries, downloads, applications, videos, photographs, and electronic documentation in the cellular telephone's memory. In addition, I know that a forensic examination of a cellular telephone and these other devices can result in the retrieval of such data which has been stored on them, even after the passage of time, because files that have been hidden or deleted can still be recovered.

8. Based upon training, knowledge, and experience as well as from information obtained from other law enforcement officers, I know that it is common practice for drug traffickers to routinely utilize cell phones, text messaging apps, and coded communications to interact with and do business with their customers, suppliers, confederates, and couriers. I also know that drug traffickers utilize multiple cell phones to evade law enforcement detection and that drug traffickers utilize firearms in furtherance of their illegal activities. Therefore, I know that evidence of drug crimes can be found in electronic media such as cell phones. Such evidence

includes, but is not limited to addresses, telephone numbers, email and texts to confederates involved in the drug trade. Moreover, it is not uncommon for drug traffickers to photographs of themselves and others involved in the drug trade. I am aware that drug-related searches of mobile devices have resulted in the recovery of photographs of defendants in possession of firearms, which are tools of the drug trade; large amounts of currency; and drugs. When these "trophy photos" are taken and/or retained, such photographs can be used as evidence or can lead to evidence of additional drug trafficking and associated offenses such as money laundering. As with most electronic/digital technology, communications made from or to an electronic device are often stored on the device itself. Moreover, as technology progresses, the distinction between computers and cell phones is becoming less clear. Accordingly, in addition to electronic communications, cell phones also contain information pertaining to a user's internet activities. A forensic examiner can recover evidence that shows when and in what manner a user of an electronic device utilized such a device.

9. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the internet. Even when such files have been deleted, they can be retrieved through the use of forensic tools. When a file on an electronic device is "deleted," the data contained in the file does not actually disappear, but remains on the device until it is overwritten by new data. Therefore, deleted files or the remnants of deleted files, may reside in free space or slack space—that is, in space on a device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary internet directory or "cache." The

browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from an electronic storage device depends less on when the file was sent, downloaded, or viewed than a particular user's operating system, storage capacity, and habits.

10. Finally, based upon training, knowledge, and experience as well as from information obtained from other law enforcement officers, I know that the following types of evidence have been recovered through the execution of warrants in drug trafficking investigations related to cell phones and other electronic communication devices: (1) contact lists, including telephone numbers and contact information; (2) incoming and outgoing calls; (3) incoming and outgoing text messages; (4) photographs; (5) videos; (6) instant messaging; (7) communications via messaging apps; (8) internet search history; and (9) emails.

11. I am aware, based upon my training and experience, that the following kinds of evidence have been recovered in a substantial number of cellular telephone & computer searches executed in connection with drug trafficking and money laundering investigations:

a. Contact lists, including telephone numbers and names associated with those numbers;

b. Incoming and outgoing call logs;

c. Incoming and outgoing text messages, including draft text messages;

d. Photographs and/or videos;

e. Emails;

f. Online/social media postings; and

g. Banking information.

12. My awareness of these drug trafficking practices, as well as my knowledge of drug

use and distribution techniques as set forth in this Affidavit, arise from the following: a) my involvement in prior drug investigations and searches during his career, as previously described; b) my involvement on a number of occasions in debriefing confidential informants and cooperating individuals in prior drug investigations, as well as what other agents and police officers have advised me of when relating the substance of their similar debriefings and the results of their own drug investigations; c) discussions with members of the FBI and/or other federal, state, and local law enforcement officers, both about the facts of this case in particular and about trafficking in general; and d) other intelligence information provided through law enforcement channels.

13. Based on the facts set forth in this Affidavit, I submit there is probable cause to believe that the **TARGET DEVICE** contains evidence of the TARGET OFFENSES. Because this Affidavit is being submitted for the limited and specific purpose of supporting an application for a search warrant for the **TARGET DEVICE**, I have not included every fact known to law enforcement concerning this investigation. I have not, however, omitted any facts that would tend to defeat a finding of probable cause.

III. PROBABLE CAUSE

Title III Wiretap Investigation

14. On March 7, 2024, the Honorable William S. Stickman IV, United States District Court Judge for the United States District Court for the Western District of Pennsylvania, signed an Order authorizing initial interceptions over (412) 892-1704, utilized by Cayce WILLIAMS, for a period of thirty days, at Misc. No. 24-234(a). The thirty-day period for interceptions on (412) 892-1704 ended on April 5, 2024.

15. On April 5, 2024, the Honorable Robert J. Colville, United States District Judge for the United District Court for the Western District of Pennsylvania, signed an Order authorizing

the initial interceptions over (412) 606-2236, utilized by Malik MARTINEZ, for a period of thirty days, at Misc. No. 24-234(c). The thirty-day period for the interceptions of (412) 606-2236 ended on May 4, 2024.

16. On April 10, 2024, the Honorable Robert J. Colville, United States District Judge for the United District Court for the Western District of Pennsylvania, signed an Order authorizing the continued interceptions over (412) 892-1704, utilized by Cayce WILLIAMS, for a period of thirty days, at Misc. No. 24-234(c). The thirty-day period for the interceptions of (412) 892-1704 ended on May 9, 2024.

17. On May 9, 2024, the Honorable William S. Stickman IV, United States District Judge for the United District Court for the Western District of Pennsylvania, signed an Order authorizing the continued interceptions of (412) 606-2236 and the initial interceptions of (412) 608-5756, both of which are utilized by Malik MARTINEZ, for a period of thirty days, at Misc. No. 24-234(d). The thirty-day period for the interceptions of and (412) 606-2236 and (412) 608-5756 ended on June 7, 2024.

18. On June 18, 2024, the Honorable William S. Stickman IV, United States District Judge for the United District Court for the Western District of Pennsylvania, signed an Order authorizing the continued interceptions of (412) 606-2236, utilized by Malik MARTINEZ, for a period of thirty days, at Misc. No. 24-234(e). The thirty-day period for the interceptions of (412) 606-2236 ended on July 17, 2024.

19. This investigation is targeting a local Drug Trafficking Organization (DTO), with which I believe Cayce WILLIAMS (WILLIAMS) and Malik MARTINEZ are associated. WILLIAMS, MARTINEZ and other members of the DTO, distribute heroin/fentanyl and cocaine

in and around the Allentown neighborhood of Pittsburgh, Pennsylvania ("Allentown"), specifically in and around the area of East Warrington Avenue.

20. **Cayce WILLIAMS**, date of birth ("DOB") June 13, 2002, a/k/a "Smooth", a/k/a "CM", ("CAYCE WILLIAMS"), is a member of the Organization who obtains quantities of heroin/fentanyl and crack cocaine for distribution throughout the Allentown, Beltzhoover, and Knoxville sections of Pittsburgh. I have reviewed CAYCE WILLIAMS' criminal history through a query of the NCIC. CAYCE WILLIAMS does not have any criminal convictions; however, he has several arrests that have been dismissed and several pending cases. In March 2022, CAYCE WILLIAMS was arrested for Simple Assault, but was not prosecuted. On September 22, 2023, CAYCE WILLIAMS was arrested for Possession of a Controlled Substance with Intent to Deliver or Delivery of a Controlled Substance, Possession of a Controlled Substance, and Possession of Drug Paraphernalia. Prosecution is pending for this matter. On November 27, 2023, CAYCE WILLIAMS was arrested for Possession of a Controlled Substance. Prosecution is pending for this matter. All of CAYCE WILLIAMS' arrests were in Allegheny County, Pennsylvania.

21. **Malik MARTINEZ**, DOB: November 21, 1996, a/k/a "Leek", a/k/a "Paco", ("MARTINEZ"), is a member of the Organization who obtains quantities of heroin/fentanyl and crack cocaine for distribution throughout the Allentown, Beltzhoover, and Knoxville sections of Pittsburgh. I have reviewed MARTINEZ's criminal history through a query of the NCIC and learned that he has a prior federal conviction. On November 7, 2019, MARTINEZ was convicted of Conspiracy to Distribute Quantities of Fentanyl, Heroin, and Crack Cocaine, and one count of Possessing a Firearm in Furtherance of Drug Trafficking Crime. MARTINEZ was sentenced to seventy-two months in federal prison followed by three years' supervised release. MARTINEZ has several state convictions. Significantly, on October 24, 2018, MARTINEZ pleaded guilty to

Possession of a Controlled Substance with Intent to Deliver or Delivery of a Controlled Substance and was sentenced to twelve months' county probation. All of MARTINEZ's state convictions were in the Allegheny County Court of Common Pleas.

22. Law enforcement has determined that CAYCE WILLIAMS utilizes 304 Kathleen St., Pittsburgh, PA 15211 as his primary residence based on the following information:

23. First, since approximately March 2024, law enforcement has observed CAYCE WILLIAMS at 304 Kathleen St. on a near daily basis.

24. Second, investigators queried CAYCE WILLIAMS' Pennsylvania Identifications through the Pennsylvania Department of Motor Vehicles and learned that his address is listed as 304 Kathleen St., Pittsburgh, PA 15211.

25. Third, during several occasions during the interception period of TARGET TELEPHONE 1, CAYCE WILLIAMS provided his address. For example, on March 10, 2024, at approximately 10:57 p.m., CAYCE WILLIAMS sent an outgoing text message to Leslie Spinelli, utilizing (412) 482-7748, where he provided his name and address ("304 Kathleen st 15211 cayce Williams").

Williams - Narcotics Distribution Based on TIII Wire Interceptions

26. On March 9, 2024, law enforcement intercepted communications between Malik MARTINEZ, utilizing (412) 606-2236 ("TARGET TELEPHONE 3") and WILLIAMS, utilizing (412) 892-1704.

27. During interceptions of (412) 892-1704, utilized by WILLIAMS, and (412) 265-7501, utilized by Malik MARTINEZ law enforcement confirmed that Malik MARTINEZ supplied CAYCE WILLIAMS with narcotics.

28. For example, on May 6, 2024, at approximately 9:10 a.m., CAYCE WILLIAMS, utilizing (412) 892-1704, placed an outgoing call to Malik MARTINEZ, utilizing (412) 608-5756. A transcribed portion of the call is as follows (CW – Cayce Williams; MM – Malik Martinez):

> MM: Yo.
> CW: Where you at?
> MM: Yo.
> CW: Huh?
> MM: Yo cuz.
> CW: Where you at?
> MM: Who's this?
> CW: CM, nigga!
> MM: Dude...I-I'll be back in like, ten minutes.
> CW: Fuck. I was gonna say, put that thirty in the mailbox, bro. I'll grab some more tickets.

29. Based on training and experience, your Affiant believes CAYCE WILLIAMS, utilizing (412) 892-1704 placed an outgoing call to Malik MARTINEZ, utilizing (412) 608-5756, to establish a narcotics transaction. After greeting each other, CAYCE WILLIAMS asks Malik MARTINEZ where he is ("Where you at?"). Malik MARTINEZ questions who was calling him ("Who's this?"). CAYCE WILLIAMS responds by stating that it is CM ("It's CM, nigga!"). Malik MARTINEZ tells CAYCE WILLIAMS that he will be back in ten minutes ("Dude…I-I'll be back in like, ten minutes."). CAYCE WILLIAMS stated that he wanted more narcotics and directed Malik MARTINEZ to leave a quantity of unknown narcotics in his mailbox for CAYCE WILLIAMS to retrieve ("Fuck. I was gonna say, put that thirty in the mailbox, bro. I'll grab some more tickets.").

30. Your Affiant believes CAYCE WILLIAMS, utilizing (412) 892-1704, was supplied unknown narcotics by Malik MARTINEZ, utilizing (412) 608-5756.

31. Additionally, on July 10, 2024, from 3:07 a.m. to 3:24 a.m., MARTINEZ, utilizing TARGET TELEPHONE 3, had the following text message exchange with CAYCE WILLIAMS, utilizing (412) 463-4855. The text messages are as follows (MM – Malik Martinez; CW – Cayce Williams):

MM: U smacking
CW: Naw
MM: Whatttttt? I got 3 over here
CW: I'm coming over u got new port
MM: It's almost 4 I got a physical at 8 not going to sleep (crying emoji)
……
CW: Open the door
MM: Negative my girl sleep quiz stop
CW: My bad
MM: Disrespectful
CW: Quiz my bad

32. Based on training and experience, your Affiant believes MARTINEZ, utilizing TARGET TELEPHONE 3, and CAYCE WILLIAMS, utilizing (412) 463-4855, had a text message conversation where MARTINEZ told CAYCE WILLIAMS he had narcotics at his residence. MARTINEZ asked CAYCE WILLIAMS if he had any ecstasy (MDMA) ("U smacking") and CAYCE WILLIAMS replied in the negative ("Naw"). MARTINEZ told CAYCE WILLIAMS that he had three at his residence ("Whatttttt? I got 3 over here"). CAYCE WILLIAMS told MARTINEZ that he's coming over and asked if he had Newport cigarettes ("I'm coming over u got new port"). MARTINEZ replied that it's almost 4:00 a.m. and said he's not going to sleep because he has a physical at 8:00 a.m. ("It's almost 4 I got a physical at 8 not going to sleep (crying emoji)"). Later in the conversation, CAYCE WILLIAMS told MARTINEZ to open the door to his residence ("Open the door"). MARTINEZ replied in the negative and said his girlfriend was asleep ("Negative my girl sleep quiz stop"). CAYCE WILLIAMS apologized, and MARTINEZ admonished him.

33. Based on training and experience, your Affiant believes that WILLIAMS continued to participate in ongoing narcotics trafficking activity. For example, based on toll analysis, WILLIAMS,

utilizing (412) 463-4855, participated in 108 telephonic communications with Malik MARTINEZ, utilizing TARGET TELEPHONE 3, between July 16, 2024, and July 19, 2024.

Search Warrant – 304 Kathleen St., Pittsburgh, PA 15211 and the Body of Cayce Williams

34. On July 18, 2024, the Honorable Christopher Brown, United States Magistrate Judge for the Western District of Pennsylvania, signed a search warrant for the person of Cayce WILLIAMS, as well as the residence of WILLIAMS at 304 Kathleen St., Pittsburgh, PA 15211.

35. On July 19, 2024, at approximately 6 a.m., members of FBI Pittsburgh SWAT team knocked and announced their presence at the residence. FBI Pittsburgh SWAT took WILLIAMS into custody without incident. FBI Pittsburgh SWAT informed agents on scene that WILLIAMS looked at them out of a window inside of the living room, prior to exiting the residence upon SWAT call-out. While in custody of FBI Pittsburgh SWAT, WILLIAMS informed agents that his phone was left inside of the living room prior to exiting 304 Kathleen Street.

IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

37. There is probable cause to believe that things that were once stored on the **TARGET DEVICE** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because

when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

V. FORENSIC EVIDENCE: DELETED FILES; USER ATTRIBUTION

38. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **TARGET DEVICE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks

and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to distribute controlled substances and to communicate with suppliers and customers involved in the purchase and sale of controlled substances, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

VI. NATURE OF EXAMINATION AND MANNER OF EXECUTION

39. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **TARGET DEVICE** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **TARGET DEVICE** to human inspection in order to determine whether it is evidence described by the warrant.

40. Manner of execution. Because this warrant seeks only permission to examine the **TARGET DEVICE** already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VII. CONCLUSION

41. Based upon the foregoing, there is probable cause to conclude that, in the Western District of Pennsylvania and elsewhere, WILLIAMS has engaged in violations of the TARGET

OFFENSES. There is probable cause to believe that evidence of these crimes will be found upon searching the above **TARGET DEVICE**.

The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

/s/ Samantha Keener
Samantha Keener, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 24th day of July, 2024.

HONORABLE PATRICIA L. DODGE
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The item to be searched is:

TARGET DEVICE: Black Cloud Mobile Cellular Phone

The Target Device will be charged and powered on. The device(s) and all readable and searchable contents will be downloaded to a "CelleBrite" or "XRY" or similar device. The contents downloaded on the "CelleBrite" or "XRY" or similar device will then be copied to a readable computer disc and reviewed by your Affiant or other investigators participating in the investigation. A search warrant return will be provided to the Court thereafter. The **TARGET DEVICE** are currently located in the evidence storage facilities at FBI Pittsburgh, 3311 East Carson Street, Pittsburgh, Pennsylvania 15203, and are stored in a manner that is designed to preserve the electronic data.

ATTACHMENT B

Property to be Seized

II. CELLULAR TELEPHONES

1. All records on cellular telephones that relate to violations of Title 21, United States Code, Sections 841, 843(b), and 846 and Title 18, United States Code, Sections 922(g)(1) and 924(c) including:

a. Evidence of communications referring to or relating to illegal narcotics or narcotics trafficking, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

b. Evidence of communications with suppliers, purchasers, prospective suppliers, or prospective purchasers of illegal narcotics, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

c. Evidence of communications referring to or relating to firearms and/or ammunition, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

d. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, or ammunition;

e. Documents, including video and/or audio recordings, discussing and/or referring to illegal narcotics, drug paraphernalia, firearms, or ammunition;

f. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, ammunition, violence relating to firearms or ammunition;

g. Any and all information revealing the identity of co-conspirators in drug trafficking and/or firearm-related activity;

h. Any and all bank records, transactional records, records of wire transfers, checks, credit card bills, account information, and other financial records;

i. Any and all information suggesting sudden or unexplained wealth and/or unidentified conspirators;

j. Any and all information identifying the sources of supply and/or unidentified conspirators may have secured illegal narcotics, drug paraphernalia, firearms, and/or ammunition; and

k. Any and all information recording the scheduling of travel and/or unidentified conspirators, including destinations, dates of travel, and names used during travel.

2. All text messaging, call logs, emails, and/or other records of communication relating to the planning and operation of drug trafficking, misuse of communications facilities, illegal possession of firearms, and possession of firearms in furtherance of drug trafficking crimes, in violation of 21 U.S.C. §§ 841, 843(b), and 846 and 18 U.S.C. §§ 922(g)(1) and 924(c).

3. Evidence of user attribution showing who used, owned, or controlled the cellular telephones at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

4. Evidence of software that would allow others to control the cellular telephones, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

5. Evidence of the lack of such malicious software.

6. Evidence indicating how and when the cellular telephones were accessed or used to determine the chronological context of the cellular telephones access, use, and events relating to the crimes under investigation and to the cellular telephones user.

7. Evidence indicating the cellular telephones user's state of mind as it relates to the crime under investigation.

8. Evidence of the attachment to the cellular telephones of other storage devices or similar containers for electronic evidence.

9. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the cellular telephones.

10. Evidence of the times the cellular telephones were used.

11. Evidence of how the cellular telephones were used and the purpose of its use including firewall logs, caches, browsing history, cookies, "bookmarked" or "favorite" web pages, temporary Internet directory or "cache," search terms that the user entered into any Internet search engine, records of user-typed web addresses, and other records of or information about the cellular telephones' Internet activity.

12. Records of or information about Internet Protocol addresses used by the cellular telephones.

13. Passwords, encryption keys, and other access devices that may be necessary to access the cellular telephones.

14. Documentation and manuals that may be necessary to access the cellular telephones or to conduct a forensic examination of the cellular telephones.

15. Contextual information necessary to understand the evidence described in this attachment.

16. All serial numbers or International Mobile Equipment Identity (IMEI) numbers associated with any cellular telephones.

17. Log files, contact information, phone books, voicemails, text messages, draft messages, other stored communication, calendar entries, videos, and photographs related to matters described above.

In searching the cellular telephones, and during the execution of these search warrants, law enforcement is permitted to: (1) depress WILLIAM's thumb- and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of WILLIAMS' face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force; specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

In searching the cellular telephones, the federal agents may examine all of the information contained in the cellular telephones to view their precise contents and determine whether the cellular telephones and/or information fall within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden," or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any of the following:

a. Any form of computer or electronic storage (such as hard disks or other media that can store data);

b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;

c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;

d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e*. friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e*. date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents,

downloads, status, translations, shared information, GPS, mapping, and other information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Any information related to co-conspirators (including names, addresses, telephone numbers, or any other identifying information);

i. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

j. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files, downloads, purchase history, photographs, videos, links, calendar information, settings, home page information, shared history and/or information, printed history and/or information, or location data;

k. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of operating a sophisticated fraud scheme, or other criminal violations;

l. Any handmade form (such as writing);

m. Any mechanical form (such as printing or typing); and

n. Any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).